UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/029,349	12/28/2001	Leon Hurst	004770.00756	5493

22907 7590 10/24/2006		EXAMINER
BANNER & WITCOFF		ZAND, KAMBIZ
1001 G STREET N W		

ART UNIT	PAPER NUMBER
2132	

SUITE 1100
WASHINGTON, DC 20001

DATE MAILED: 10/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/029,349	HURST ET AL.
	Examiner	**Art Unit**	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
 Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>27 September 2006</u>.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,16-21 and 84-104* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *84* is/are allowed.

6)☒ Claim(s) *1-5,16-21,85-91,93,95-102 and 104* is/are rejected.

7)☒ Claim(s) *92,94 and 103* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All   b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.

2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

3. Claims 6-15, and 22-83 have been cancelled.

4. Claims 1, 16, 17, 84, 90, and 92 have been amended.

5. new claims 95-104 have been added.

6. Claims 1-5, 16-21 and 84-104 are pending.

7. The objections of claims 6-10 are moot due to cancellation of claims 6-10 by the applicant(s).

8. The double patenting rejection of claim 77 is moot due to cancellation of claims 76-77 by the applicant(s). .

Response to Arguments

9. Applicant's arguments with respect to claim 1 is not persuasive for the following reasons:

 • Personal trusted device is not a device that belong to a particular user based on item 21 fig.7 of applicant's drawings and associated texts, but a device for holding users certificates and verification process of any user that have a

corresponding stored user certificate. Demotto disclose such device as applied to rejection of claim below. If applicant claiming that such device is only assigned to one user and that is why it is called a personal trusted device in contradiction to fig.7 of the applicant specification, then examiner request a corresponding drawings of claim 1 that discloses such claim be shown by applicant, if not, then such a claim, and limitation "personal trusted device" based on the arguments presented raise 112 first paragraph enablement issue since the specification do not give support for such claim in clear manner.

- As for applicant's arguments with respect to claims 85-86, the use of PDA, wireless technology is inherent in PDA technology. Also col.8, lines 6-32 also disclose the network may be a WAN using a Internet and having remote capabilities, low powered radio frequency is also inherent part of PDA (a simple search of "PDA definition" in Google would disclose such inherency in number of ways).

- Applicant has not provided arguments with respect to dependent claims 2-5 and 85-89, and therefore their rejections are maintained based on applicant's unpersuasive arguments with respect to claim 1 as it was outlined above. Applicant's insistence on "wireless interface" or "low power radio frequency interface" are not persuasive as DeMello et al disclose such limitations as

outlined above. Examiner reminds applicant to concentrate the arguments

over the inventive steps or novelty of applicant's invention over prior art.

Limitation "wireless interface" or "low power radio frequency" is not a novel or

an inventive steps as it would be recognized by one of ordinary skilled in the

art and more particularly the core of applicant's invention (please do a basic

search with respect to PDA, wireless interface definition in Google).

- Applicant's arguments with respect to MPEP 2114 and Ex Parte Mashem

  case, that addresses apparatus is a semantic arguments similar to the absent

  of wireless technology in PDA that are not persuasive. The Case is related to

  an apparatus, however the content and the concept of the ruling has to do

  with that the intended use of a concept that has been implemented in the past

  as prior art, has no novelty or an inventive steps, and therefore unpatentable.

  That is if a process, a method of prior art has a capability to perform, then the

  intended use of it in a claim does not distinguishes it over the prior art of such

  process or method. The applicant's arguments therefore not persuasive and

  the rejections of the claims are maintained.

- **Applicant's arguments are persuasive in the light of limitations of**

  claims 84, 92, 94 and 103, and further in light of applicant's

  specification. Therefore rejections of the above claims have been

  withdrawn (see allowability subject matter below).

10. Applicant's arguments with respect to the new added claims 95-102 and 104

   have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

11. **Claims 101-103** are objected to because of the following informalities: A claim

   cannot depend on itself, possible typo error. Examiner suggests the dependency

   of claim 101 be changed to claim "100". Appropriate correction is required.

12. Claims 102-103 will have a correct dependency upon the correction of claim 101.

13. **Claim 96** is objected to under 37 CFR 1.75(c), as being of improper dependent

   form for failing to further limit the subject matter of a previous claim. Applicant is

   required to cancel the claim(s), or amend the claim(s) to place the claim(s) in

   proper dependent form, or rewrite the claim(s) in independent form. The use of

   the phrase "one or more" does not further limits the claim since claim 1 already

   deals with transmission to "one" device. The phrase "or" give the option of choice

   between "one" or "more", and the choice of "one" do not further limits the claim.

   Examiner has chosen limitation "one" for the purpose of examination. **Examiner**

   suggests the phrase "two or more" as a proper further limiting limitation in

   light of limitations of claim 1.

Claim Rejections - 35 USC § 102

14. **Claims 1-10, 16-27, 84-88, 92, 96, 97, 99, 100, 101, and 104** are rejected under

35 U.S.C. 102(e) as being anticipated by DeMello et al (6,891, 953 B1).

As per claims 1 and 96 DeMello et al (6,891, 953 B1) teach a method of decrypting

encrypted content stored on a terminal, the method comprising the steps of: **receiving a**

request to access encrypted content on a terminal (see col.2, lines 4-8 where it

disclosed the protected content are encrypted in harmony with col.3, lines 18-33

where a request for such access is being disclosed); obtaining a license comprising

a content decryption key (see col.6, lines 46-53) and a set of binding attributes, the

attributes including a public key (see col.6, lines 36-67; col.7, lines 1-2) **of an**

authorized user of the encrypted content (see col.6, lines 42-45 where examiner

considers the user activation certificate corresponding to applicant's "the

authorized user"); in response to the request, polling a personal trusted device of said

user to digitally sign data with a private key associated with the device **(see col.11,**

lines 48-55 where examiner considers the server corresponding to applicants

personal trusted device use the private key of the fulfillment center which is the

database of the server provider and is associated with the sever to sign); receiving

said digitally signed data from said device **(see col.11, lines 50-67; col.12, lines 1-17**

where data is received and authenticated); and verifying at the terminal the digitally

signed data utilizing the said public key; and wherein the terminal in response to

verification of the digitally signed data uses the content decryption key to decrypt the

encrypted content **(see fig.2-4 and associated text; col.11, lines 43-67; col.8, lines 1-6; col.21, lines 36-67; col.22-28; col.33, lines 28-67 disclose all above limitations including certification of the license with user's attributed including the keys, verification of signed certificate; hashing verification to tamperproof the content and communication between the two parties including the decryption of the content by the receiver by decryption key).**

As per claims 2 DeMello et al (6,891, 953 B1) teach a method as claimed in claim 1 comprising: encrypting at least the content decryption key (see col.2, lines 22-30; col.6, lines 38-46 where the decryption key which is the same as encrypted key because they are symmetric keys are encrypted).

As per claim 3 DeMello et al (6,891, 953 B1) teach a method as claimed in claim 2, wherein: encryption is performed using a public key of an asymmetric key pair such that decryption of the content decryption key is carried out using a private key of the asymmetric key pair (see col.2, lines 61-67;col.3, lines 1-2;col.6, lines 10-21 and col.11, lines 49-57).

As per claim 4 DeMello et al (6,891, 953 B1) teach a method as claimed in claim 3, wherein: the private key is stored in a tamperproof and secure location (see col.6, lines 10-21;col.10, lines 30-44 and col.11, lines 33-44).

As per claims 5 and 18 DeMello et al (6,891, 953 B1) teach a method, a terminal as

claimed in claims 4, 17 respectively, wherein: the secure location comprises a security

element (see col.14, lines 7-16 where the ids corresponds to applicant's security

elements).

As per claim 16 DeMello et al (6,891, 953 B1) teach a terminal which renders

encrypted content comprising:

a storage for the encrypted content and a license (see col.6, lines 45-47 the DRAM and

53-67), the license containing a content decryption key and a set of binding attributes,

the attributes including a public key for a licensee of said content (see col.6, lines 36-67;

col.7, lines 1-2);

a protected processing environment (see fig.1 and associated text; col.1, lines 60-67);

a network interface which, in response to said terminal receiving a request to access

said stored encrypted content (see fig.2 and associated text; see col.2, lines 1-61),

establishes a communication link between the terminal and at least one other terminal

(see fig.2 and associated text) to request the other terminal to encrypt and digitally sign

identity verification data using a private key stored at the other terminals and which

delivers the digitally signed identity verification data received from the other terminal to

the protected processing environment (see fig.2-4 and associated text; col.11, lines 43-

67; col.8, lines 1-6; col.21, lines 36-67; col.22-28; col.33, lines 28-67 disclose all above

limitations including certification of the license with user's attributed including the keys,

verification of signed certificate; hashing verification to tamperproof the content and

communication between the two parties including the decryption of the content by the

receiver by decryption key); and

wherein the protected processing environment uses said public key to decrypt said

encrypted identity verification data, compares said decrypted data with said digital

signature to verify the digitally signed data, and upon successful verification of the

digitally signed data, the protected processing environment decrypts the encrypted

content using the content decryption key (see fig.7-8 and associated text and as applied

to claim 1 above).

As per claim 17 DeMello et al (6,891, 953 B1) teach a terminal as claimed in claim 16,

comprising: a tamperproof and secure storage for private key of an asymmetric key pair:

and wherein the protected processing environment decrypts at least the content

decryption key, the content decryption key having been encrypted using a public key of

the asymmetric key pair (see col.2, lines 22-30 and 61-67;col.3, lines 1 and 2;col.6,

lines 10-21 and 30-44; col.11, lines 33-57).

As per claims 19-21 DeMello et al (6,891, 953 B1) teach a terminal as claimed in

claims 16, 17 and 18 respectively, wherein: the digitally signed identity verification data

is delivered to the storage (see col.6, lines 45-47 and 53-67 DRAM).

As per claims 85-86, 97, 99 and 104 DeMello disclose communication via network

interface as disclosed in fig.1-4 and associated text including using wireless interface.

Also see Col.5, lines 58-63 disclose using such device as PDA, Pocket PC where wireless technology and low power radio frequency is inherent. A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)).

As per claim 87 DeMello et al (6,891, 953 B1) teach the method of claim 1, wherein said terminal is rendering machine, and said method further includes a step of rendering said decrypted content on said rendering machine (see col.6-9).

As per claims 88 and 89 DeMello et al (6,891, 953 B1) teach the method of claim 1, further comprising the steps of receiving an identification of a user making said request; and comparing said identification with a public portion of said license (see col.2, lines 50-61; col.5, lines 23-27; and fig.1-8 and associated text see databases).

As per claim 100-101 DeMello et al (6,891, 953 B1) teach all limitations of the claims as applied to claims 1 and 16 above.

Claim Rejections - 35 USC § 103

15. **Claims 90-91, 93 and 102** are rejected under 35 U.S.C. 103(a) as being unpatentable over DeMello et al (6,891, 953 B1) in view of Rosen (5,557,518).

DeMello disclose all limitation of the claims as applied to the claims above but do not expressly disclose random generation of the data. However Rosen (5,557,518 A) teach random generation of the data by a device (see fig.9b and associated text). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rosen's random number generator device in DeMello's secure content distribution in order to have customer communication and authentication in a secure manner by changing the authentication parameters randomly.

Allowable Subject Matter

16. **Claim 84** has been allowed.

17. **Claims 92, 94 and 103** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

19. Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Kambiz Zand whose telephone number is (571)

272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone

numbers for the organization where this application or proceeding is assigned as

571-273-8300. Information regarding the status of an application may be

obtained from the Patent Application Information Retrieval (PAIR) system. Status

information for published applications may be obtained from either Private PAIR

or Public PAIR. Status information for unpublished applications is available

through Private PAIR only. For more information about the PAIR system, see

http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197

(toll-free).

KAMBIZ ZAND
PRIMARY EXAMINER

10/22/2006

AU 2132